UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/665,805	09/18/2003	David Anthony Cook	112025-0533	6624

24267 7590 06/26/2008

CESARI AND MCKENNA, LLP
88 BLACK FALCON AVENUE
BOSTON, MA 02210

EXAMINER	
MESFIN, YEMANE	
ART UNIT	PAPER NUMBER
2144	
MAIL DATE	DELIVERY MODE
06/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/665,805	**Applicant(s)** COOK, DAVID ANTHONY
	Examiner Yemane Mesfin	**Art Unit** 2144

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _01 April 2008_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1,2,4-17 and 19-33_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1,2,4-6,8-14,16,17,19, 21-28 and 30-33_ is/are rejected.

7)☒ Claim(s) _7,15, 20 and 29_ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _18 September 2003_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04/01/2008 has been entered. Claims 1, 2, 4-17, and 19-33 are pending.

Response to Arguments

2. Applicant's arguments filed 04/01/2008 have been fully considered but they are not persuasive.

The inventive entity recites:

- ***Chen is Disqualified as Prior Art under 35 U.S.C. § 103(a) by Operations of 35 U.S.C. § 103(C)…Chen was previously assigned to Cisco Technology, Inc****. by an assignment recorded at Reel/Frame 010002/0505 on May 27, 1999* ***(Remarks, Page 13).***
- ***35 U.S.C. § 103(c) is satisfied since Chen does not qualify as § 102(a)****, (b), (c) or (d) prior art.*
  35 U.S.C. § 102(a) states a person is entitled to a patent unless "the invention... was patented or described in a printed publication .... before the invention thereof by the applicant." Chen was first published on Apr. 22ha, 2003 when it issued as a patent. ***The Applicant files herewith a Declaration Under 35 C.F.R. 1.131 establishing conception of the invention prior to Apr. 22nd, 2003 and diligence until reduction to practice****. As a result of such Declaration Under 35 C.F.R.1. 131, Chen to not qualify as prior art under §102(a)* ***(See Remarks, Page 14, ¶¶ 1-2).***

3. Examiner respectfully disagrees. Chen remains qualified prior art under 35 U.S.C. § 102(a), thus applicable under **35 U.S.C. § 103(a),** because applicant's Declaration under 35 C.F.R. 1.131 and the supporting evidence is deficient for several reasons. Therefore, the declaration is not efficient to properly disqualify Chen as a prior art. **See rationale disclosed below with respect to the Declaration Under 35 C.F.R. 1.131**.

Affidavit or Declaration under 37 CFR 1.131

4. The affidavit filed on **04/01/2008** under 37 CFR 1.131 has been fully considered. However, it is ineffective to properly disqualify **Chen** as a prior art reference under the qualification of **35 U.S.C. § 103(c) [(i.e., to show common assignee to avoid an obviousness rejection** under **35 U.S.C. § 103(a))]**. The evidence submitted is insufficient to establish diligence from a date prior to the **effective publication date of Chen** (i.e., prior to April 22, 2003) to the date of reduction to practice, either actual or constructive (in this case the filing this US Patent Application, filed on September 18, 2003).

The affidavit and the accompanying Exhibit A merely demonstrate prior conception. In the first place, the Declaration fails to properly map each and every limitations of the claimed invention to the supporting evidential provided (i.e., the exhibit A). Applicant's declaration simply points to the summary section of the submitted Exhibit A (see Declaration, Page 2, Line 5). Second, there is absolutely no time line of any activity showing due diligence. Rather, the documents relied upon shows period of inactivity from a date prior to the effective publication date of Chen and to the date of constructive reduction to practice of this instant application.

Where conception occurs prior to the date of the reference (in this case prior to the publication date of Chen, since the purpose of this declaration is merely to satisfy the requirement of U.S.C. § 103(c)), but reduction to practice is afterward, it is not enough merely to allege that applicant or patent owner had been diligent. Ex parte Hunter, 1889 C.D. 218, 49 O.G. 733 (Comm'r Pat. 1889). Rather, applicant must show evidence of facts establishing diligence.

What is meant by diligence is brought out in Christie v. Seybold, 1893 C.D. 515, 64 O.G. 1650 (6th Cir. 1893). In patent law, an inventor is either diligent at a given time or he is not diligent;

there are no degrees of diligence. An applicant may be diligent within the meaning of the patent law when he or she is doing nothing, if his or her lack of activity is excused. Note, however, that the record must set forth an explanation or excuse for the inactivity; the USPTO or courts will not speculate on possible explanations for delay or inactivity. See In re Nelson, 420 F.2d 1079, 164 USPQ 458 (CCPA 1970). Diligence must be judged on the basis of the particular facts in each case. See MPEP § 2138.06 for a detailed discussion of the diligence requirement for proving prior invention. Under 37 CFR 1.131, the critical period in which diligence must be shown begins just prior to the effective date of the reference (the publication date of Chen in this case, since the declaration is merely to satisfy the requirement of U.S.C. § 103(c)**)** or activity and ends with the date of a reduction to practice, either actual or constructive (i.e., filing a United States patent application).

An applicant must account for the entire period during which diligence is required. Gould v. Schawlow, 363 F.2d 908, 919, 150 USPQ 634, 643 (CCPA 1966) (Merely stating that there were no weeks or months that the invention was not worked on is not enough.); In re Harry, 333 F.2d 920, 923, 142 USPQ 164, 166 (CCPA 1964) (statement that the subject matter "was diligently reduced to practice" is not a showing but a mere pleading). **A 2-day period lacking activity has been held to be fatal**. In re Mulder, 716 F.2d 1542, 1545, 219 USPQ 189, 193 (Fed. Cir. 1983) (37 CFR 1.131 issue); Fitzgerald v. Arbib, 268 F.2d 763, 766, 122 USPQ 530, 532 (CCPA 1959) (Less than 1 month of inactivity during critical period. Efforts to exploit an invention commercially do not constitute diligence in reducing it to practice).

Thus, Chen is qualified prior art, because the evidence provided is ineffective to properly disqualify the Chen patent by satisfying the requirements of **35 U.S.C. § 103(c)**. Accordingly all pending claims 1, 2, 4-17, and 19-33 are now rejected under 35 U.S.C. 103(a) as being unpatentable over Chen (U.S. Patent Number 6,553,423) in view of Gill et al., ("The BGP TTL Security Hack (BTSH")

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 8-11 and 21-24 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 8 and 21 call for system adapted to…, the system [1] comprising: routing protocol process executing in a router… (See claims 8 and 21).

However, an ordinary skill in the art could interpret the system to be an entirely software program (software per se). As recited in the claim, the system comprising "routing protocol process executing in a router…" implies an executable program per se. Thus, "routing protocol process executing in a router", unless shown to be tangibly stored in computer readable **storage** (emphasis added) media/medium, is non statutory. Evidently, the inventive entity recites, "…it is expressly contemplated that the teachings of this invention, including the various processes described herein, can be implemented as **software**" (see Specification Page 17, Lines 4-5).

Therefore, since the claims may be interpreted to mean entirely software as disclosed above, the claims are rejected as being directed to a non statutory subject matter. It should be noted that a system claim lacking specific hardware arrangements and/or a combination of both hardware and

[1] Note: In this case, it is the examiners opinion that a system claim should comprise at lest one peer router (i.e., the one or more peer router devices involved in the system as recited in the claim), and the "routing protocol process" should be stored in a computer-readable storage medium in order to cure the problem.

software components for realizing the claimed invitation does not fall in any categories of process, machine, manufacture or composition of matter so to be given a patentability weight. Consequently, Claims 8-11 and 21-24 are now rejected under 35 U.S.C. 101 because the claims are directed to a non-statutory subject matter.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 2, 4-6, 8-14, 16, 17, 19, 21-28, and 30-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen (U.S. Patent Number 6,553,423) in view of Gill et al., ("The BGP TTL Security Hack (BTSH").

As per claim 1, Chen disclosed a method for allowing a router to efficiently determine a time-to-live (TTL) configuration of a peer router in a computer network [Abstract, and Column 3, Lines 10-36, determination of router's routing capabilities and Column 6, Lines 18-19 ("...a technique for dynamically exchanging or updating routing capabilities between neighboring peer routers in a computer network..."], the method comprising the steps of: automatically determining which TTL mode of operation the peer router supports by sending an initial Border Gateway Protocol (BGP) message [Chen, Column 6, Lines 41-43, via BGP] from the router to the peer router, the initial BGP message including a first predetermined value of a TTL parameter [Column 3, Lines 10-36, dynamically announcing and updating of capabilities among routers and

Column 5, Lines 7-21, …interdomain routers ("neighboring peer routers") exchanging routing and reachability information…one of the neighboring peer routers sending a message… and Column 5, Lines 25-29, …the message including therein predetermined parameters specified by the peer routers, the parameter field being a capability parameter introducing new features that may be supported by a peer router]; if the router receives a positive acknowledgement of the initial BGP message from the peer router, determining that the peer router supports exchanges of messages using a new TTL mode of operation; if the router receives a negative acknowledgement of the initial message from the peer router, deciding that the peer router does not support the new TTL mode of operation [Column 5, Line 20 through Column 6, Line 43, pointing by reference to a "capability negotiation with BGP-4", which address the operation of a BGP speaker router determining capability of it's peer router via a NOTIFICATION including error subcode set to Unsupported Capability, which is received from the peer router and accordingly, determining if the peer router supports the new capability and if it does not support the new capability, re-sending another message with a different optional capability parameter]; and switching to an old capability mode of operation by resending the initial message with a second predetermined value of the TTL parameter [Column 6, Lines 4-65, replacing to a previously (old) announced capability].

Chen substantially disclosed the invention and further taught that the initial message is Border Gateway Protocol (BGP) routing protocol message [Column 6, Lines 41-43]. However, Chen was silent about new capability parameter being a time-to-live (TTL) parameter.

However, as evidenced by the teachings of Gill, a time-to-live (TTL) parameter, defined by BGP TTL Security Hack (BTSH) was known in the art at the time the invention was made [see, Gill et al. Internet draft, <draft-gill-btsh-02.txt>, published on May 2003, Abstract through § 4 (Security Considerations)]. Thus, it is respectfully submitted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to take the teachings of Gill related to BGP TTL Security Hack (BTSH) and have modified the teachings of Chen in order "to protect the BGP … infrastructure from CPU-utilization based attacks and provide a lower level of protection to multi-hop sessions" (see Gill et al., Abstract and § Introduction).

As per claim 2, the already combined teachings of Chen and Gill disclosed the invention as recited above in claim 1, wherein the step of deciding comprises the step of, if the router does not receive a response at all within a predetermined time, deciding that the peer router does not support the new TTL mode of operation [Gill Abstract through § 4 (Security Considerations) reciting TTL mode of operations and Chen Column 5, Lines 20-64, where Chen disclosed determination of a peer router incapability when a peer router fails to reply to the message initiated by the router].

As per claim 4, the already combined teachings of Chen and Gill disclosed the invention as recited above in claim 1, wherein the new TTL mode of operation is defined by BGP TTL Security Hack (BTSH)[Gill Title, and Abstract through § 4 (Security Considerations), TTL mode of operation is defined by BGP TTL Security Hack (BTSH)].

As per claim 5, the already combined teachings of Chen and Gill disclosed the invention as recited above in claim 1, wherein the first predetermined value of the TTL parameter capability is 255 [Gill, Page 4, § BTSH Procedure, … where the TTL mode is in the range of 255-254 for peer to peer routers] .

As per claim 6, the already combined teachings of Chen and Gill disclosed the invention as recited above in claim 1, wherein the second predetermined value of the TTL parameter is 1 [The TTL parameter 1 is the typical value of the a TTL parameter that does not support the new TTL mode. As further shown in Gill, Page 3, § 2.1. Assumptions on Attack Sophistication, TTL parameter 1].

As per claim 8, a system adapted to allow a router to efficiently determine a time-to-live (TTL) configuration of a peer router in a computer network [Abstract, and Column 3, Lines 10-36, determination of router's routing capabilities and Column 6, Lines 18-19 ("…a technique for dynamically exchanging or updating routing capabilities between neighboring peer routers in a computer network…"], the system comprising: a routing protocol process executing in the peer router and adapted to receive an initial routing protocol message sent by an initiating routing protocol process executing in the router, the initial routing protocol message including a predetermined value of a TTL parameter[Column 5, Line 20 through Column 6, Line 43, pointing to a "capability negotiation with BGP-4", which address the operation of a BGP speaker router determining capability of it's peer router via a NOTIFICATION including error subcode set to Unsupported Capability, which is received from the peer router and accordingly, determining if the peer router supports the new capability and if it does not support the new capability, re-sending another message with a different optional capability parameter], the routing protocol process returning one of (i) a positive acknowledgement of the initial routing protocol message to the router if the peer router supports exchanges of messages using a new TTL mode of operation and (ii) a negative acknowledgement of the initial routing protocol message if the peer router does not support the new TTL mode of operation [Column 5, Line 20 through Column 6, Line 43, pointing to a "capability negotiation with BGP-4", which address the operation of a BGP speaker router determining capability of it's peer router via a NOTIFICATION including error subcode set to Unsupported Capability, which is received from the peer router and accordingly, determining if the peer router supports the new capability and if it does not support the new capability, re-sending another message with a different optional capability parameter].

Chen substantially disclosed the invention and further taught that the initial message is Border Gateway Protocol (BGP) routing protocol message [Column 6, Lines 41-43]. However, Chen was silent about new capability parameter being a time-to-live (TTL) parameter.

However, as evidenced by the teachings of Gill, a time-to-live (TTL) parameter, defined by BGP TTL Security Hack (BTSH) was known in the art at the time the invention was made [see, Gill et al. Internet draft, <draft-gill-btsh-02.txt>, published on May 2003, Abstract through § 4 (Security Considerations)]. Thus, it is respectfully submitted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to take the teachings of Gill related to BGP TTL Security Hack (BTSH) and have modified the teachings of Chen in order "to protect the BGP … infrastructure from CPU-utilization based attacks and provide a lower level of protection to multi-hop sessions" (see Gill et al., Abstract and § Introduction).

As per claim 9, the already combined teachings of Chen and Gill disclosed the invention as recited above in claim 8, wherein the routing protocol process executing in the peer router implements Border Gateway Protocol version 4 (BGP) routing protocol [Chen, Column 5, Lines 10-45, capability negotiation with BGP-4].

As per claim 10, the already combined teachings of Chen and Gill disclosed the invention as recited above in claim 9 wherein the new TTL mode of operation is defined by BGP TTL Security Hack (BTSH) [Gill Title, and Abstract through § 4 (Security Considerations), TTL mode of operation is defined by BGP TTL Security Hack (BTSH)].

As per claim 11, the already combined teachings of Chen and Gill disclosed the invention as recited above in claim 10 wherein the predetermined value of the TTL parameter is 255 [Gill, Page 4, § BTSH Procedure, … where the TTL mode is in the range of 255-254 for peer to peer routers].

As per claim 12, Apparatus [Column 4, Lines 25-45, computer device (router)] adapted to allow a router to efficiently determine a time-to-live (TTL) configuration of a peer router in a computer network [Abstract, and Column 3, Lines 10-36, determination of router's routing capabilities and Column 6, Lines 18-19 ("…a technique for dynamically exchanging or updating routing capabilities between neighboring peer routers in a computer network…"], the apparatus comprising: means for sending an initial <u>Gateway Protocol (BGP)</u> message [Chen, Column 6, Lines 41-43, via BGP] from the router to the peer router, the initial message including a first predetermined value of a TTL parameter[Column 3, Lines 10-36, (dynamically announcing and updating of capabilities among routers) and Column 5, Lines 7-21, (…interdomain routers ("neighboring peer routers") exchanging routing and reachability information…one of the neighboring peer routers sending a message…); and Column 5, Lines 25-29, (…the message including therein predetermined parameters specified by the peer routers, the parameter field being a capability parameter introducing new features that may be supported by a peer router)]; means for determining that the peer router supports exchanges of messages using a new TTL mode of operation, if the router receives a positive acknowledgement of the initial BGP message from the peer router; if the router receives a positive acknowledgement of the initial BGP message from the peer router; means for deciding that the peer router does not support the new TTL mode of operation, if the router receives a negative acknowledgement of the initial BGP message from the peer router [Column 5, Line 20 through Column 6, Line 43, pointing by reference to a "capability negotiation with BGP-4", which address the operation of a BGP speaker router determining capability of it's peer router via a NOTIFICATION including error subcode set to Unsupported Capability, which is received from the peer router and accordingly, determining if the peer router supports the new capability and if it does not support the new capability, re-sending another message with a different optional capability parameter]and means for switching to an old TTL mode of operation by resending the initial message with a second predetermined value of the capability [Column 6, Lines 4-65, replacing to a previously (old) announced capability].

Chen substantially disclosed the invention and further taught that the initial message is Border Gateway Protocol (BGP) routing protocol message [Column 6, Lines 41-43]. However, Chen was silent about new capability parameter being a time-to-live (TTL) parameter and if a new TTL mode of operation is supported.

However, as evidenced by the teachings of Gill, a time-to-live (TTL) parameter, and a new TTL mode of operation defined by BGP TTL Security Hack (BTSH) was known in the art at the time the invention was made [see, Gill et al. Internet draft, <draft-gill-btsh-02.txt>, published on May 2003, Abstract through § 4 (Security Considerations)]. Thus, it is respectfully submitted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to take the teachings of Gill related to BGP TTL Security Hack (BTSH) and have modified the teachings of Chen in order "to protect the BGP … infrastructure from CPU-utilization based attacks and provide a lower level of protection to multi-hop sessions" (see Gill et al., Abstract and § Introduction).

As per claim 13, the already combined teachings of Chen and Gill disclosed the invention as recited above in claim 12 wherein the means for deciding comprises means for deciding that the peer router does not support the new TTL mode of operation, if the router does not receive a response at all within a predetermined time [Gill Abstract through § 4 (Security Considerations) reciting TTL mode of operations and Chen Column 5, Lines 20-64, where Chen disclosed determination of a peer router incapability when a peer router fails to reply to the message initiated by the router, where the predetermined time is implicitly disclosed].

As per claim 14, the already combined teachings of Chen and Gill substantially disclosed the invention as recited, wherein the new TTL mode of operation is defined by BGP TTL Security Hack (BTSH) [Gill Title, and Abstract through § 4 (Security Considerations), TTL mode of operation is defined by BGP TTL Security Hack (BTSH)].

As per claim 16, A computer readable medium [2]containing executable program instructions for allowing a router to efficiently determine a time-to-live (TTL) configuration of a peer router in a computer network [Column 8, Lines 35-51, a computer readable medium…, and Column 3, Lines 10-36, determination of router's routing capabilities and Column 6, Lines 18-19 ("…a technique for dynamically exchanging or updating routing capabilities between neighboring peer routers in a computer network…"], the executable program instructions comprising program instructions for: automatically determining which TTL mode of operation the peer router supports by sending an initial message from the router to the peer router, the initial message including a first predetermined value of a TTL parameter [Column 3, Lines 10-36, dynamically announcing and updating of capabilities among routers and Column 5, Lines 7-21, …interdomain routers

[2] Note: The **computer readable medium** recited in claim 16 is interpreted to mean a storage medium (a computer readable storage medium) as defined in the specification Page 10, Lines 15-28. There is no clear evidence in the specification, which indicates an intention to include a non statutory subject matter by means of the "computer readable medium" recited in the claim.

("neighboring peer routers") exchanging routing and reachability information…one of the neighboring peer routers sending a message… and Column 5, Lines 25-29, …the message including therein predetermined parameters specified by the peer routers, the parameter field being a capability parameter introducing new features that may be supported by a peer router]; if the router receives a positive acknowledgement of the initial BGP message from the peer router, determining that the peer router supports exchanges of messages using a new TTL mode of operation; if the router receives a negative acknowledgement of the initial BGP message from the peer router, deciding that the peer router does not support the new TTL mode of operation[Column 5, Line 20 through Column 6, Line 43, pointing by reference to a "capability negotiation with BGP-4", which address the operation of a BGP speaker router determining capability of it's peer router via a NOTIFICATION including error subcode set to Unsupported Capability, which is received from the peer router and accordingly, determining if the peer router supports the new capability and if it does not support the new capability, re-sending another message with a different optional capability parameter]; and switching to an old TTL mode of operation by resending the initial BGP message with a second predetermined value of the TTL parameter[Column 6, Lines 4-65, replacing to a previously (old) announced capability].

Chen substantially disclosed the invention and further taught that the initial message is Border Gateway Protocol (BGP) routing protocol message [Column 6, Lines 41-43]. However, Chen was silent about new capability parameter being a time-to-live (TTL) parameter and if a new TTL mode of operation is supported.

However, as evidenced by the teachings of Gill, a time-to-live (TTL) parameter, and a new TTL mode of operation defined by BGP TTL Security Hack (BTSH) was known in the art at the time the invention was made [see, Gill et al. Internet draft, <draft-gill-btsh-02.txt>, published on May 2003, Abstract through § 4 (Security Considerations)]. Thus, it is respectfully submitted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to take the teachings of Gill related to BGP TTL Security Hack (BTSH) and have modified the teachings of Chen in order "to protect the BGP … infrastructure from CPU-utilization based attacks and provide a lower level of protection to multi-hop sessions" (see Gill et al., Abstract and § Introduction).

As per claim 17, the already combined teachings of Chen and Gill substantially disclosed the invention as recited, wherein the program instruction for deciding comprises one or more program instructions for, if the router does not receive a response at all within a predetermined time, deciding that the peer router does not support the new TTL mode of operation [Gill Abstract through § 4 (Security Considerations) reciting TTL mode of operations and Chen Column 5, Lines 20-64, where Chen disclosed determination of a peer router incapability when a peer router fails to reply to the message initiated by the router].

As per claim 19, the already combined teachings of Chen and Gill substantially disclosed the invention as recited, wherein the new TTL mode of operation is defined by BGP TTL Security Hack (BTSH) [Gill Title, and Abstract through § 4 (Security Considerations), TTL mode of operation is defined by BGP TTL Security Hack (BTSH)].

As per claim 21, Chen disclosed a system adapted to allow a router to efficiently determine a time-to-live (TTL) configuration of a peer router in a computer network [Abstract, and Column 3, Lines 10-36, determination of router's routing capabilities and Column 6, Lines 18-19 ("…a technique for dynamically exchanging or updating routing capabilities between neighboring peer routers in a computer network…"], the system comprising: an initiating routing protocol process executing in the router and adapted to send an initial routing protocol message to a routing protocol process executing in the peer router, the initial routing protocol message including a predetermined value of a TTL parameter [Column 3, Lines 10-36, dynamically announcing and updating of capabilities among routers and Column 5, Lines 7-21, …interdomain routers ("neighboring peer routers") exchanging routing and reachability information…one of the neighboring peer routers sending a message… and Column 5, Lines 25-29, …the message including therein predetermined parameters specified by the peer routers, the parameter field being a capability parameter introducing new features that may be supported by a peer router], the initiating routing protocol process receiving one of (i) a positive acknowledgement of the initial routing protocol message if the peer router supports exchanges of messages using a new TTL mode of operation and (ii) a negative acknowledgement of the initial routing protocol message if the peer router does not support the new TTL mode of operation [Column 5, Line 20 through Column 6, Line 43, pointing by reference to a "capability negotiation with BGP-4", which address the operation of a BGP speaker router determining capability of it's peer router via a NOTIFICATION including error subcode set to Unsupported Capability, which is received from the peer router and accordingly, determining if the peer router supports the new capability and if it does not support the new capability, re-sending another message with a different optional capability parameter].

Chen substantially disclosed the invention and further taught that the initial message is Border Gateway Protocol (BGP) routing protocol message [Column 6, Lines 41-43]. However, Chen was silent about new capability parameter being a time-to-live (TTL) parameter and if a new TTL mode of operation is supported.

However, as evidenced by the teachings of Gill, a time-to-live (TTL) parameter, and a new TTL mode of operation defined by BGP TTL Security Hack (BTSH) was known in the art at the time the invention was made [see, Gill et al. Internet draft, <draft-gill-btsh-02.txt>, published on May 2003, Abstract through § 4 (Security Considerations)]. Thus, it is respectfully submitted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to take the teachings of Gill related to BGP TTL Security Hack (BTSH) and have modified the teachings of Chen in order "to protect the BGP … infrastructure from CPU-utilization based attacks and provide a lower level of protection to multi-hop sessions" (see Gill et al., Abstract and § Introduction).

As per claim 22, the already combined teachings of Chen and Gill substantially disclosed the invention as recited in the system of claim 21 wherein the initiating routing protocol process executing in the router implements Border Gateway Protocol version 4 (BGP) routing protocol[Chen, Column 5, Lines 10-45, capability negotiation with BGP-4].

As per claim 23, the already combined teachings of Chen and Gill substantially disclosed the invention as recited in the system of claim 22, wherein the new TTL mode of operation is defined by BGP TTL Security Hack (BTSH) [Gill Title, and Abstract through § 4 (Security Considerations), TTL mode of operation is defined by BGP TTL Security Hack (BTSH)].

As per claim 24, the already combined teachings of Chen and Gill substantially disclosed the invention as recited in the system of claim 23 wherein the predetermined value of the TTL parameter is 255 [Gill, Page 4, § BTSH Procedure, … where the TTL mode is in the range of 255-254 for peer to peer routers].

As per claim 25, Chen disclosed a method comprising: sending an initial message to a peer router before a session is established with the peer router, the initial message including a first predetermined value of a time- to-live (TTL) parameter in a field that is outside of a routing protocol that makes use of the TTL parameter[Column 3, Lines 10-36, dynamically announcing and updating of capabilities among routers and Column 5, Lines 7-21, …interdomain routers ("neighboring peer routers") exchanging routing and reachability information…one of the neighboring peer routers sending a message… and Column 5, Lines 25-29, …the message including therein predetermined parameters specified by the peer routers, the parameter field being a capability parameter introducing new features that may be supported by a peer router]; if a positive acknowledgement of the initial message is received from the peer router, determining that the peer router supports exchanges of messages using a new TTL mode of operation; if a negative acknowledgement of the initial message is received from the peer router, deciding that the peer router does not support the new TTL mode of operation [Column 5, Line 20 through Column 6, Line 43, pointing by reference to a "capability negotiation with BGP-4", which address the operation of a BGP speaker router determining capability of it's peer router via a NOTIFICATION including error subcode set to Unsupported Capability, which is received from the peer router and accordingly, determining if the peer router supports the new capability and if it does not support the new capability, re-sending another message with a different optional capability parameter] and switching to an old TTL mode of operation by resending the initial message with a second predetermined value of the TTL parameter [Column 6, Lines 4-65, replacing to a previously (old) announced capability].

Chen substantially disclosed the invention and further taught that the initial message is Border Gateway Protocol (BGP) routing protocol message [Column 6, Lines 41-43]. However, Chen was silent about new capability parameter being a time-to-live (TTL) parameter and if a new TTL mode of operation is supported.

However, as evidenced by the teachings of Gill, a time-to-live (TTL) parameter, and a new TTL mode of operation defined by BGP TTL Security Hack (BTSH) was known in the art at the time the invention was made [see, Gill et al. Internet draft, <draft-gill-btsh-02.txt>, published on May 2003, Abstract through § 4 (Security Considerations)]. Thus, it is respectfully submitted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to take the teachings of Gill related to BGP TTL Security Hack (BTSH) and have modified the teachings of Chen in order "to protect the BGP … infrastructure from CPU-utilization based attacks and provide a lower level of protection to multi-hop sessions" (see Gill et al., Abstract and § Introduction).

AS per claim 26, the already combined teachings of Chen and Gill substantially disclosed the invention as recited, wherein deciding further comprises, if a response is not received within a predetermined time, deciding that the peer router does not support the new TTL mode of operation[Gill Abstract through § 4 (Security Considerations) reciting TTL mode of operations and Chen Column 5, Lines 20-64, where Chen disclosed determination of a peer router incapability when a peer router fails to reply to the message initiated by the router].

As per claim 27, the already combined teachings of Chen and Gill substantially disclosed the invention as recited, wherein the initial message is a Border Gateway Protocol (BGP) routing protocol message [Chen, Column 5, Lines 10-45, capability negotiation with BGP-4].

As per claim 28, the already combined teachings of Chen and Gill substantially disclosed the invention as recited, wherein the new TTL mode of operation is a BGP TTL Security Hack (BTSH) [Gill Title, and Abstract through § 4 (Security Considerations), TTL mode of operation is defined by BGP TTL Security Hack (BTSH)].

As per claim 30, apparatus comprising: a processor configured to execute an initiating routing protocol process [Column 4, Lines 24-45, a router comprising CPU] , the initiating routing protocol process configured to send an initial routing protocol message to a routing protocol process of a peer router before a session is established with the peer router, the initial routing protocol message including a predetermined value of a time-to- live (TTL) parameter in a field that is outside of a routing protocol that makes use of the TTL parameter[Column 3, Lines 10-36, dynamically announcing and updating of capabilities among routers and Column 5, Lines 7-21, …interdomain routers ("neighboring peer routers") exchanging routing and reachability information…one of the neighboring peer routers sending a message… and Column 5, Lines 25-29, …the message including therein predetermined parameters specified by the peer routers, the parameter field being a capability parameter introducing new features that may be supported by a peer router], and wherein the initiating routing protocol process is further configured to receive one of (i) a positive acknowledgement of the initial routing protocol message if the peer router sup\-ports exchanges of messages using a new TTL mode of operation and (ii) a negative acknowledgement of the initial routing protocol message if the peer router does not support the new TTL mode of operation, and in response to a negative acknowledgement of the initial routing protocol message [Column 5, Line 20 through Column 6, Line 43, pointing by reference to a "capability negotiation with BGP-4", which address the operation of a BGP speaker router determining capability of it's peer router via a NOTIFICATION including error subcode set to Unsupported Capability, which is received from the peer router and accordingly, determining if the peer router supports the new capability and if it does not support the new capability, re-sending another message with a different optional capability parameter], switch to an old TTL mode of operation and resend the initial message with another predetermined value of the TTL parameter [Column 6, Lines 4-65, replacing to a previously (old) announced capability].

Chen substantially disclosed the invention and further taught that the initial message is Border Gateway Protocol (BGP) routing protocol message [Column 6, Lines 41-43]. However, Chen was silent about new capability parameter being a time-to-live (TTL) parameter and if a new TTL mode of operation is supported.

However, as evidenced by the teachings of Gill, a time-to-live (TTL) parameter, and a new TTL mode of operation defined by BGP TTL Security Hack (BTSH) was known in the art at the time the invention was made [see, Gill et al. Internet draft, <draft-gill-btsh-02.txt>, published on May 2003, Abstract through § 4 (Security Considerations)]. Thus, it is respectfully submitted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to take the teachings of Gill related to BGP TTL Security Hack (BTSH) and have modified the teachings of Chen in order "to protect the BGP … infrastructure from CPU-utilization based attacks and provide a lower level of protection to multi-hop sessions" (see Gill et al., Abstract and § Introduction).

As per claim 31, wherein the initiating routing protocol process is further configured to, if a response is not received within a predetermined time, decide that the peer router does not support the new capability-TTL mode of operation [Gill Abstract through § 4 (Security Considerations) reciting TTL mode of operations and Chen Column 5, Lines 20-64, where Chen disclosed determination of a peer router incapability when a peer router fails to reply to the message initiated by the router].

As per claim 32, the already combined teachings of Chen and Gill substantially disclosed the invention as recited, wherein the initiating routing protocol process is a Border Gateway Protocol version 4 (BGP) routing protocol process [Chen Column 5, Line 20 through Column 6, Line 43, "capability negotiation with BGP-4"].

As per claim 33, the already combined teachings of Chen and Gill substantially disclosed the invention as recited, wherein the new TTL mode of operation is defined by BGP TTL Security Hack (BTSH) **[**Gill Title, and Abstract through § 4 (Security Considerations), TTL mode of operation is defined by BGP TTL Security Hack (BTSH)**]**.

Allowable Subject Matter

9. Claims 7, 15, 20 and 29 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yemane Mesfin whose telephone number is (571) 272-3927. The examiner can normally be reached on 9:00 AM - 6:00 PM Mon - Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William C. Vaughn can be reached on (571) 272-3922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Yemane Mesfin/
Examiner, Art Unit 2144